Wave Systems Corp
480 Pleasant Street
Lee, MA 01238
Tel: 413-243-1600; Fax: 413-243-4500
www.wave.com

wave

January 17, 2007

Federal Trade Commission
Office of the Secretary
Room H-135 (Annex N)
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580

Dear Sir or Madam:

Re: Identity Theft Task Force, P065410

Recently, the Federal Identity Theft Task Force issued a public request for comments on the protection of consumer privacy, identity, and data security. After reading the interim recommendations and the request for comments, we submit the following comments for your consideration.

1: Replacing Social Security Numbers
While it is irrefutable that removal of personally identifiable information (PII) such as Social Security Numbers from online transactions would be an improvement over the status quo, any proposed solution should recognize that PII will be inevitably used in transactions. One potential solution is to lessen the need for PII as unique identifiers by relying on authentication factors disassociated from the individual. Current technologies such as the "Trusted Platform Module" now available on virtually all shipping personal computers, allow for the creation and secure storage of digital identities with hardware-level security. Leveraging these technologies makes forgery of identities essentially impossible.

2: Protecting PII
Establishing national standards for corporate and government protection of PII, including transaction related information, would ensure consistency in the data practices and we encourage guidance and standards in this area. However, these standards and policies should leverage the existing work of the trusted computing group. Tremendous investment has been made by industry to ensure all PC's will have a common identity and security infrastructure that can be leverage by any industry world wide. Broad adoption is already underway by the DOD.

The FTC should leverage these commercial-off-the-shelf specifications solutions and industry standards to provide a framework for a secure digital future. Recommendations can simply outline best practices already present: financial services and healthcare companies should support strong authentication, and be required to secure customer information using hardware – the only real way to achieve security. Every new business PC has this capability built in and consumer adoption is expected in 2008.

The recent large-scale loss of consumer data due to laptop theft cries for more specific guidance on protecting "Data at Rest" on these and other mobile devices. Hardware technology is rapidly advancing, and Full Disk Encryption hardware is now available which would effectively solve the "lost laptop" problem once and for all. These hardware based solutions have virtually no impact on the performance of information systems, are inexpensive, and offer phenomenal security benefits.

3: Technology leadership
The federal government should lead. All e-government infrastructure should support strong authentication with Trusted Platform Modules. The result would be a return on investment would be both rapid and substantial: stronger international leadership, better data security for the American people, protection of critical systems, and American investment in an important business sector.

The federal government has made the decision to support Public Key encryption as a baseline for intra-government data security. But it's difficult to mandate PKI for all industry and local interactions. This is where the Trusted Computing Group and other standards group can help. By creating standards that have been adopted worldwide by the PC manufacturers and by Intel and Microsoft, the TCG has accomplished what the federal government can't. Every first responder, every police department every municipality, and every hospital has (or soon will) PCs with this hardware security built in. A common, worldwide framework for secure communication and data protection is emerging right in front of us. It's important for the US to take a leadership role in *how it's used.*

Wave Systems would be glad to discuss these issues, either in public forum or confidentially, should that be constructive to your efforts.

Sincerely,

Steven Sprague
President/CEO

SKS:ls

Cc Senator E Kennedy
Senator J Kerry
Congressman J Olver